KHIE
KENTUCKY HEALTH INFORMATION EXCHANGE

Five things I wish I knew 10 years ago

Richard Chapman, JD
Chief Privacy Officer
University of Kentucky HealthCare

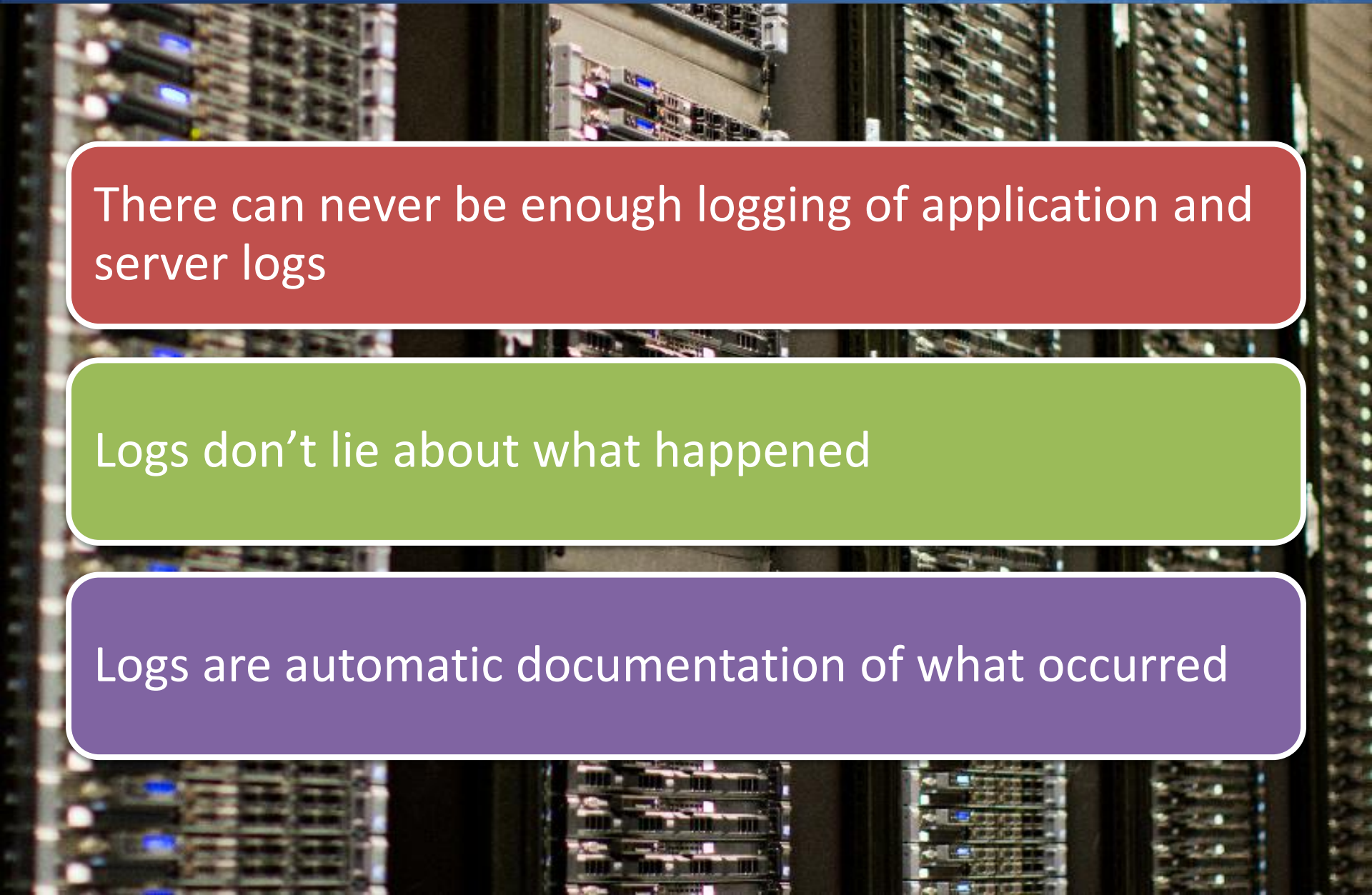
Karen Chrisman JD MA
Privacy Officer/Staff Attorney
Division of Kentucky Electronic Health Information

Kentucky
UNBRIDLED SPIRIT

2015 “The Year of the Breach?”

ORGANIZATION	RECORDS	TYPE	INDUSTRY	SCORE
ANTHEM INSURANCE COMPANIES (ANTHEM BLUE CROSS) (U.S.)	78,800,000	IDENTITY THEFT	HEALTHCARE	10.0
GENERAL DIRECTORATE OF POPULATION AND CITIZENSHIP AFFAIRS/THE GENERAL DIRECTORATE OF LAND REGISTRY AND CADASTER (TURKEY)	50,000,000	IDENTITY THEFT	GOVERNMENT	9.9
U.S. OFFICE OF PERSONNEL MANAGEMENT (U.S.)	21,000,000	IDENTITY THEFT	GOVERNMENT	9.6
TOPFACE (RUSSIA)	20,000,000	ACCOUNT ACCESS	TECHNOLOGY	9.2
GAANA.COM / TIMES INTERNET (PAKISTAN)	10,000,000	IDENTITY THEFT	RETAIL	8.9
RAKUTEN AND LINE CORP (JAPAN)	7,850,000	ACCOUNT ACCESS	RETAIL	8.8
TALKTALK (U.K.)	4,000,000	IDENTITY THEFT	OTHER	8.8
MEDICAL INFORMATICS ENGINEERING (U.S.)	3,900,000	IDENTITY THEFT	HEALTHCARE	8.8
ADULT FRIENDFINDER (U.S.)	3,867,997	EXISTENTIAL DATA	OTHER	8.6
REGISTER.COM (U.S.)	1,400,000	EXISTENTIAL DATA	TECHNOLOGY	8.5
SAUDI ARABIA GOVERNMENT (SAUDI ARABIA)	1,000,000	EXISTENTIAL DATA	GOVERNMENT	8.4

Logging of Application and Server Logs



There can never be enough logging of application and server logs

Logs don’t lie about what happened

Logs are automatic documentation of what occurred

Managing the Breach

Talk to the leader early

Establish expectations and deadlines

There will be plenty of time to disagree later

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule

Decision Team Before the Incident

- Taking the time to set up a decision team before the incident is worth the effort
- Incidents are usually out of sight out of mind
- Have a defined team who can make decisions and interpret applicable regulations

Media Release

Media Release Template ready

- Required for 90 days for individuals without a mailing address
- Easier to edit than draft
- Use your contacts with local media
- https://www.nomoreclipboard.com/notice

Collect and Organize Documentation

Taking time to collect and organize documentation after an incident is worth the effort

There is never enough time to properly document after an incident.

Documentation cannot be organized as well 3 months after the incident

KHIE
KENTUCKY HEALTH INFORMATION EXCHANGE

Phishing Incidents

Value of Encrypted email

Once encrypted always encrypted

Audit Documentation

HHS OCR auditor's are more concerned about documentation proof than actually protecting the patient's information

OCR follows a standard checklist that is designed to meet OCR's needs

No auditor ever asks you to explain your own process to address an incident

Insider Threat

Insider Threat is a current of former employee, contractor or business partner who:

- Has or had authorized access to an organization's network, system, or data
- Has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability (CIA) of the organization's information or information systems

Most common insider crimes:

- Unauthorized access
- Unintentional exposure of private or sensitive data
- Viruses, worms or other malicious code
- Theft of intellectual property

Sometimes you just can't figure out exactly what happened

Lack of logging often helps reach this conclusion

Conflicting human stories can also lead to a non-conclusion